North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: McKenna Long & Aldridge

Address: 1900 K Street, NW
Washington, DC 20006-1102
Telephone: 202-496-7500
Fax: 202-496-7756
Email:

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: Initial letter sent 02/28/2014; Form submitted on 03/13/2014

Date the Security Breach was discovered: MLA was notified of suspicious activity on February 14, 2014, by its vendor, but was not able to confirm a breach until on or about February 18, 2014.

Estimated number of affected individuals: 1,301

Estimated number of NC residents affected: 9

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b): Ultimate Performance

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Information related to current and former MLA employees was accessed on November 28, 2013, December 11, 2013 and December 12, 2013

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: The information is password protected and users must sign in with a user ID and password to gain access.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: MLA has reset all passwords for each user and asked all users to establish a new password. We are also working with our vendor to ensure that this does not occur again.

Date affected NC residents were/will be notified: February 27, 2014

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding

the delay pursuant to N.C.G.S. § 75-65(a) and (c)): N/A

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?
(pursuant to N.C.G.S. § 75-65(e))
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

- ☒ written notice
- ☐ electronic notice (email)
- ☐ telephone notice
- ☐ substitute notice

Signature: _____ Date: _____

Contact Person, Title: Raymond O. Aghaian
Address: 300 S. Grand Avenue, 14th Floor, Los Angeles, CA 90071
(if different from above) _____
Telephone: 213-688-1000 Fax: 213-243-6330 Email: raghaian@mckennalong.com

USW 804362419.2

Albany
Atlanta
Brussels
Denver
Los Angeles
New York

McKenna Long & Aldridge LLP
300 South Grand Avenue • 14th Floor
Los Angeles, CA 90071-3124
Tel: 213.688.1000
mckennalong.com

Orange County
Rancho Santa Fe
San Diego
San Francisco
Washington, DC

RAYMOND O. AGHAIAN
Direct Phone: 213.243.6160
Direct Fax: 213.243.6330

EMAIL ADDRESS
raghaian@mckennalong.com

February 28, 2014

CONFIDENTIAL COMMUNICATION
VIA FEDERAL EXPRESS

Consumer Protection Division
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001

Re: Data Breach Notification

Dear Consumer Protection Division:

In accordance with N.C. Gen. Stat. §75-65 et seq., we are sending this letter to inform you of a data breach involving information of current and former employees of the law firm of McKenna Long & Aldridge LLP ("MLA"), which was stored and maintained by an outside vendor.

As explained in the enclosed notification letter, the vendor notified MLA of the suspicious activity on February 14, 2014 and MLA immediately began investigating this incident. In the course of the investigation, MLA reviewed records, to include system access activity log files, system access user identification and password logs, Internet Protocol addresses used for access, the information elements associated with each access, discussed the incident on several occasions with the vendor, interviewed an MLA employee, and reset all user passwords for the affected database. MLA also continues to work with the vendor to discover additional information that may be relevant to determining the cause of the incident and how to prevent such breaches in the future.

Please find enclosed a sample of the notification that was sent to North Carolina residents on February 27, 2014. MLA believes approximately Nine (9) North Carolina residents were affected by the incident.

Very truly yours,

Raymond O. Aghaian

ROA/JAS
Enclosure

USW 804323629.1

February 26, 2014

Dear [NAME],

McKenna Long & Aldridge ("MLA") recently learned of suspicious computer activity on servers belonging to one of our vendors, which stored information about MLA's current and former employees. The vendor notified MLA of this suspicious activity on February 14, 2014 and MLA immediately began investigating this incident. As a result of that investigation and further information provided by the vendor, it appears that some information related to current and former employees was accessed on November 28, 2013 (Thanksgiving Day), December 11, 2013, and December 12, 2013 and that such access was obtained through the malicious and unauthorized access to the user identification and password of an account administrator. MLA has since reset all passwords for each user and asked all users to establish a new password. We are also working with our vendor to ensure that this does not occur again.

Regrettably, our investigation appears to show that your personal information was accessed without authorization during this incident, including Federal Wage and Tax Statement Form W-2 name, address, wages, taxes and Social Security number information; date of birth, age, gender, ethnicity; and Visa, Passport or Federal Form I 9 documents numbers. We are notifying you so that you can take action to minimize or eliminate potential harm as a result. Because this is a serious incident, we strongly encourage you to take preventive measures now to help prevent and detect any misuse of your information.

For example, as a preventive step, we recommend that you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. In the event you learn of an identity theft, you can submit a complaint with the Federal Trade Commission by calling 1 877 ID THEFT (1 877 438 4338), or through their website at https://ftccomplaintassistant.gov, or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. Moreover, you may want to contact the three United States credit reporting agencies (Equifax, Experian, and TransUnion) to obtain a credit report. Free credit reports are available to all consumers every 12 months by calling 1-877-322-8228, or by logging on to www.annualcreditreport.com. Contact information for the three credit reporting agencies is as follows:

Equifax	Experian	TransUnion
(800)525-6285	(888)397-3742	(800)680-7289
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.com

As an added precaution, MLA is providing you with one year of credit monitoring and identity theft protection at no cost to you. The service, provided by Experian, is called **ProtectMyID**. To activate these protections, simply:

1. Ensure that you enroll by May 31st, 2014
2. Call 877-371-7902 OR visit the **ProtectMyID** website: http://www.protectmyid.com/redeem
3. Provide this activation code: [redacted]

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your reports periodically can help you spot problems and address them quickly.

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it may also delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies.

We have also advised the three major United States credit reporting agencies about this incident, and have given those agencies a general report, alerting them to the fact that the incident occurred. However, we have not notified them about the presence of your particular information in the data breach.

* * *

For **residents of Iowa**, you may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319 (515) 281-5164 www.iowaattorneygeneral.gov.

For **residents of Maryland**, you may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. You can contact the Maryland Attorney General at: Office of the Attorney General, Consumer Protection Divisions, 200 St. Paul Place, Baltimore, MD 21202 (888)743-0023 www.oag.state.md.us.

For **residents of Massachusetts**, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also requires that you be informed of the following procedure in order to obtain a security freeze on your credit report: If you have been the victim of identity theft, and you provide the credit reporting agency with a valid police report, you cannot be charged to place, lift or remove a security freeze. In other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request

to each of the three major credit reporting agencies, listed below, and you must provide the following information: Full name; Social Security Number; date of birth; if you have moved in the past five years, the addresses where you have lived for the prior five years; proof of current address, such as a utility bill; a legible photocopy of a government issued identification card, such as a driver's license; if you have been the victim of identity theft, a copy of either the police report or complaint to law enforcement regarding identity theft; if you are not a victim of identity theft, payment by check, money order, or credit card. Do not send cash.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and Social Security number), as well as the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you would like the credit report to be available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

Likewise, to remove the security freeze, you must send a written request to each of the three credit reporting agencies by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze. After receiving your request, the credit reporting agencies have three business days to remove the security freeze.

For **residents of North Carolina**, you may obtain information about avoiding identity theft from the FTC or the North Carolina Attorney General's Office. You can contact the North Carolina Attorney General at: Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 (877)566-7226 http://www.ncdoj.gov/.

* * *

We want to stress that we genuinely regret any inconvenience or concern this incident may cause you.

Jeff Haidet, Chairman
McKenna Long & Aldridge LLP